LARA LICENSING AND REGULATORY AFFAIRS CUSTOMER DRIVEN. BUSINESS MINDED.	**Effective Date:**	09-12-2011
	Policy #:	H--04
	Supersedes:	
Subject: **Impermissible Use, Disclosure or Breach of Confidential or Protected Health Information – Prompt Action Required**	**Page:**	1 of 6

PURPOSE

The purpose of this policy/procedure is to inform all Department of Licensing and Regulatory Affairs (LARA) employees of the process required for prompt response to reported, suspected, or actual impermissible uses, disclosures, or breaches of confidential or protected health information.

DEFINITIONS

Breach means the unauthorized acquisition, access, use, or disclosure of confidential information or PHI that compromises the security or privacy of the confidential information of PHI.

Breach Notification is the provision of information to notify an individual about the use or disclosure of the individual's confidential information that may compromise the privacy or security of the individual as required by applicable law

Confidential Information means information of a private nature that is protected by law from public disclosure, such as identifiable health information, social security numbers, etc.

Impermissible Use or Disclosure means the acquisition, access, use, or disclosure of confidential information or PHI in a manner not permitted under HIPAA or other applicable confidentiality law that may or may not compromise the security or privacy of the confidential information or PHI.

PHI is the acronym for Protected Health Information as defined under the Health Insurance Portability and Accountability Act (HIPAA). PHI is health information that can be linked to an individual through an identifier and can be in any format: paper, verbal, electronic, etc.

LARA LICENSING AND REGULATORY AFFAIRS CUSTOMER DRIVEN. BUSINESS MINDED.	**Effective Date:**	09-12-2011
	Policy #:	H--04
	Supersedes:	

Subject: **Impermissible Use, Disclosure or Breach of Confidential or Protected Health Information – Prompt Action Required**	**Page:**	2 of 6

POLICY

LARA Director's Office and designated Privacy Officer will promptly respond to reports of actual or suspected impermissible uses, disclosures, or breaches of confidential or protected health information. Steps will be taken to investigate, mitigate, log, remedy assess or evaluate risk, notify affected individuals when required, make required reports to appropriate agencies, notify Human Resources when required, and implement corrective actions to prevent recurrence of event.

PROCEDURE

Responsibility	**Action**
Workforce member	As soon as possible report all actual or suspected impermissible uses, disclosures, or breaches of confidential or protected health information to the member's supervisor/manager and the LARA Director's Office ,Privacy Officer, and others as required. An incident report must be completed and sent to the LARA Privacy Officer as soon as possible. Please highlight the e-mail as "high priority". Workforce member will work with the Privacy Officer to investigate, mitigate, and remedy the incident.
Workforce Member's Supervisor/Manager	When supervisor/manager is made aware of the actual or suspected impermissible use, disclosure, or breach, the supervisor/manager must promptly ensure that the Privacy Officer and others are informed as required. The supervisor/manager will ensure that an incident report is completed and forwarded to the LARA Privacy Officer

	and will ensure that any involved workforce members will work with the Privacy and Officer to investigate, mitigate, and remedy the incident.
LARA Director's Office and Privacy Officer	**<u>Investigate</u>** • Collect all possible information from reporting workforce member and any other individuals with knowledge related to the incident. Collect the following information: ○ The name of the workforce member and agency having control of the confidential information or PHI ○ List of names of affected individuals ○ Type of information disclosed or accessed (Data elements) ○ The format of the information: paper, electronic, portable device ○ Whether the information was encrypted and the encryption standard used ○ Whether the information was password protected ○ Who received the information ○ Whether the information was rendered unusable or indecipherable ○ Any additional available and related ○ information **<u>Mitigate</u>** • Take immediate steps to mitigate the breach. • Identify the source of access or disclosure of confidential information or PHI

- Stop source from further access or disclosure
- If criminal activity, contact police and obtain police report

Remedy

- Log incident in central office or hospital/center database
- Notify Chief Deputy Director and area Senior Deputy Directors in case of serious breach
- Notify Human Resources when workforce member involvement as appropriate
- Evaluate and analyze the incident; identify and apply applicable confidentiality laws (e.g., Public Health Code, Mental Health Code, HIV/AIDS/STDs, Substance Abuse, HIPM-HITECH, Identity Theft Protection Act, Social Security Number Privacy Act, Medicaid, Social Welfare Act
- Perform risk assessment
- Notify individuals of breach when required by law in accordance with the previous required analysis and risk assessment
  - HIPPA and MI TEC Breach Notification applies to covered components and business associates
  - Michigan Identity Theft Protection Act breach notification provision applies to all state agencies
- Determine whether credit protection should be provided to individuals
- Notification letter must be in plain language and include:
  - Brief description of breach
  - Date of breach (if known)

	○ Date of discovery ○ Identify the data elements breached, e.g., full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc. ○ Provide information about how to protect the affected individual from harm ○ Brief description of what the agency is doing to investigate and mitigate the harm and protect against any further breaches ○ Contact information for questions - toll free phone number, email address, web site or postal address • If individuals are unknown, provide notice in accordance with applicable law. • Report breach to authorities as required by applicable law. ○ HIPM covered entities must report breaches to the director's office: ▪ if 500 or more, must report immediately ▪ if less than 500, must provide log within 60 days after the close of the calendar year ○ Medicaid agencies must report breaches to the Centers or Medicare and Medicaid regional director • Note whether any grant/contract provisions require report to grant or information source. • Determine corrective actions needed to prevent recurrence: ○ New or updated policies or procedures needed? ○ Updated or refreshed training needed? ○ Employee counseled - or sanctioned?

	○ General reminders to staff needed? ○ Or any other recommended action? • Maintain documentation/report of analysis, risk assessment, and all actions taken. ○ Under HIPM, Covered Entity has the burden of proof to show all steps that were taken for each reported incident of impermissible uses or disclosures ○ o Under HIPAA, if individual(s) are not notified, the Covered Entity must have documentation to show why notification was not required

REFERENCES

Michigan Identity Theft Protection Act, MCL 445.61 et. seq.
HIPAA and HITECH Act, 45 CFR
Alcohol and Substance Abuse 42 CFR Part 2
Michigan Substance Abuse, MCL 333.6521
Michigan Substance Abuse Confidentiality, MCL 333.6111-6113
Michigan Mental Health Code, MCL 330.1748
Michigan Public Health Code, MCL 333.1101 et. al.
HIV/Aids
Medicaid, 42 CFR 431.300-431.307